INSPECTOR GENERAL
IG 78-897

3 May 1978

DD/A Registry
78-1814/1

OGC Has Reviewed OSD review completed

MEMORANDUM FOR: Director of Central Intelligence

VIA: Deputy Director of Central Intelligence

FROM: John H. Waller
Inspector General

SUBJECT: Proposed Executive Order on Declassification

1. Action Requested:

That you seek exemptions at least equal to those in the current Executive Order 11652, if necessary, discussing the issue with the President.

2. Background:

Subject draft, dated 20 April 1978, is the latest in a series of drafts developed since last June. In keeping with the Administration's policy of openness in Government, it promotes reduced classification in Government documents and shorter time frames for automatic declassification. The DCI is mentioned only once, and then in the context of approver of "special access programs" established by Agency heads, which programs have intelligence sources and methods issues. The Secretary of Defense is authorized "to establish special procedures" for classified cryptologic information; Restricted Data information continues to be exempt, and information generated "by the President, his White House staff or Committees and Commissions appointed by the President, or others acting on his behalf," enjoys protection from mandatory declassification review for a longer period than other information, including intelligence.

3. Discussion:

This draft establishes a new Information Security Oversight Office in the General Services Administration, in accord, we understand, with the President's instruction. The DCI could be required to seek document-by-document exemptions

from the Director of this new office; appeals, if a DCI request was denied, would go to the NSC. Knowledgeable people feel that the DCI would seldom lose such a contest, but the administrative burden of reviewing every classified document now 20 years old (vice the current 30 years for national security information), would have to be added to that already required for FOIA, Privacy Act, and other such vehicles of public demand. Additional personnel, particularly in the Directorate of Operations where the issue is most sensitive, would have to be taken from their operational duties. Any citizen could request a mandatory declassification review of any document six years old or older. The authority of any authorized Top Secret classifying officer (including the DCI) to extend the protection period from six years to 20 years (or 30 years if it is "foreign government" information) ". . . shall be used sparingly."

4. The Office of the General Counsel has done yeoman's work in influencing this draft, which we gather is a considerable improvement over others. Nevertheless, it appears that some fundamentals in the intelligence business and the role of the DCI as the President's senior intelligence officer have not been understood, or accepted, by the chairman of the drafting committee.

-- Many intelligence capabilities do not have a six year or 10 year or 20 year half-life: cryptosystem attack, certain technological capabilities and long-term agent associations often extend for decades.

-- No nation with regard for its long-term security, foreign policy or intelligence-gathering interests can entertain the idea of eventual public release of the details of its foreign intelligence activities.

-- An intelligence service with a reputation for poor security and an inability to honor confidentiality becomes ineffectual.

-- The release of incremental bits of apparently innocuous data related to intelligence activities (as occurs under the FOIA and can expand under automatic declassification schemes such as proposed in subject draft) will

enhance our growing reputation for giving away secrets and permit clever adversaries to reconstruct that which we intended to keep secret in the first place.

5. This is not to say that we cannot go ahead with your commitment to make more intelligence available to others. But you should determine its releasability and format, the focus being the sharing of evaluated substantive information, not operational details or raw untested commentary from field reports.

6. Conclusion:

I consider this a serious, fundamental issue, not a bureaucratic and procedural records management issue. Having come through the prolonged investigative period and having new intelligence guidelines in Executive Order 12036, I suggest that we stand firm on fundamentals and seek exemption from procedures which treat intelligence data like any other Federal Government data.

7. Recommendations:

a. That you discuss this issue with Dr. Brzezinski and, if necessary, the President to retain, at least, the exemption authority now in Executive Order 11652.

b. That the drafting committee be instructed by Dr. Brzezinski that there are classes of intelligence documents (such as clandestine operations cables) which should never be subject to automatic declassification.

(signed)
John H. Waller

John H. Waller

Next 1 Page(s) In Document Exempt

Approved For Release 2003/08/08 : CIA-RDP81-00142R000200070006-0

OGC 78-2772

28 April 1978

MEMORANDUM FOR: Anthony A. Lapham

STATINTL FROM : [redacted]
Associate General Counsel

SUBJECT : Remaining Issues in E.O. 11652 Revision

STATINTL 1. You asked me to review Deanne Siemer's memorandum of 20 April (Tab A), together with those of Bob Gambino (Tab B) and [redacted] April 20 (Tab C), and to recommend concerning the issues remaining under the revision on which DoD and the Director/CIA seem to be in disagreement. Gambino's memorandum is a draft, for DDA signature to the Director; the DDA has not acted on the paper. [redacted] has met with DDA and DDS&T reps to consider the Siemer memorandum, and has submitted a new paper of 26 April to you (Tab D). The draft Order is at Tab E. STATINTL

STATINTL 2. Siemer's memorandum concerns section 4(e)(3) only. In his 26 April memorandum of his meeting with DDA and DDS&T, [redacted] advises that DDS&T would accept the DoD proposal on 4(e)(3), although they would like some DoD clarification. DDA on the other hand would request a change in the DoD language and George recommends this also. See Tab D, particularly paragraphs 5-7. My own view is that while I would not object to at least proposing the DDA and DDS&T points to Siemer, I think they are not important and I would not expend much standing, reputation or resources to push them, and I certainly would not push this issue up to the President, or indeed to Brzezinski or the SCC.

3. There seem to be, or to have been, two points concerning 4(e)(3):

a. Is its authority to be available only to the Secretary of Defense and DoD (NSA) components or also to the DCI and CIA?

b. Would the 4(e)(3) authority in the Secretary of Defense encroach on the DCI's authority under E.O. 12036 and if so should 4(e)(3) therefore be objected to?

4. As to the former, CIA had proposed an amendment which would confer the 4(e)(3) authority also on the DCI as to CIA. The newest draft

does not include this proposal and Deanne's letter requests that we withdraw that proposed amendment. Based on the WGJ memoranda and the Gambino paper there seems to be no disposition within CIA to ask for inclusion of the DCI/CIA in 4(e)(3). I think a reply to Siemer therefore could accede to that request.

5. As to the latter point, there is concern that the paper would take from the DCI some of his security authorities under E.O. 12036 and in effect give them to the Secretary of Defense. See Gambino's paper (Tab B). I agree with George's view that the paragraph should not be so read. Additionally, I am not persuaded that the result would be undesirable in any event, although this admittedly is not a legal point, and I think the issue is not an important one. Hence, as George proposes, I would recommend to Siemer the amendment suggested at paragraph 7 of Tab C, but not to the point of forcing a dispute to higher levels. Also, before approaching Siemer I should think you would want to reach an agreement with the DDA, in which event the memorandum to the DCI submitted for Blake's signature would not be necessary.

6. A related point, not mentioned by Siemer or Gambino--namely, the last sentence of 4(e)(3) is a non sequitor. What is "the information" which is to remain classified? The penultimate sentence of that paragraph also is awkward. Suggest both be replaced as follows:

> If the Director of the ISSO disapproves procedures or requires changes not satisfactory to the Secretary of Defense, the Secretary of Defense may appeal the matter to the NSC.

7. Gambino also objects to the provision that would except compartmentation systems which are required "by treaty or international agreement" from the automatic five-year termination. I should think the exception is desirable, at least as to existing systems. Surely we should not abrogate treaties or international agreements in this manner.

STATINTL 8. [redacted] understands Bob Gates proposes to forward the draft Order to OMB early next week. It is recommended therefore that you:

a. Discuss and reach agreement with Blake to take the positions proposed in paragaphs 4, 6 and 7; and

b. By telephone confirm with Siemer your acceptance of her 4(e)(3).

[redacted] STATINTL

Attachments
cc: EO/DDA

Approved For Release 2003/08/08 : CIA-RDP81-00142R000200070006-0

GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
WASHINGTON, D.C. 20301

April 20, 1978

OGC 78-2555
4-21-78

Anthony A. Lapham
General Counsel
Central Intelligence Agency
Washington, D. C. 20505

Dear Tony:

We view Section 4(e)(3) of the proposed Executive Order on classification of information to be a purely procedural matter that has nothing whatever to do with the division of operational responsibility in the signals intelligence area.

It was inserted in the Executive Order at our request because Section 4(e)(2) requires guidelines for a systematic review for declassification that state "specific, limited categories of information which, because of their national security sensitivity, should not be declassified automatically but should be reviewed item-by-item to determine whether continued protection beyond 20 years is needed." We tried hard to get both underlined terms taken out of Section 4(e)(2). If that had been done, we would not have needed Section 4(e)(3). As I understand it, the Domestic Council staff thought that the underlined items were so important that it would be more acceptable politically to give us an exemption than to delete the objectionable words.

We plan to issue procedures under Section 4(e)(3) that provide for continued classification beyond 20 years for all or nearly all signals intelligence and communications intelligence information and that provide for review by large category (such as source) rather than item-by-item. Any signals intelligence, communications intelligence or other classified cryptologic information in the hands of CIA or other agencies would be covered automatically by these procedures.

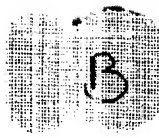
We think it is advantageous to approach the Director of the Information Security Oversight Office very soon after he or she is appointed with this blanket request. We also think it is more likely to be accepted if it comes solely from NSA and does not appear to be a Community-wide project taking advantage of a large loophole.

Our interests are identical in this area and OJ would appreciate it if CIA's proposed amendment could be withdrawn.

Sincerely,

Deanne

Deanne C. Siemer



Approved For Release 2003/08/08 : CIA-RDP81-00142R000200070006-0

ROUTING AND RECORD SHEET

SUBJECT: (Optional)

DCI Authority for SIGINT Security Policy

FROM:	EXTENSION	NO.
Robert W. Gambino Chairman, Security Committee		SECOM-D-320/1 DATE 19 APR 1973

TO: (Officer designation, room number, and building)	DATE RECEIVED	DATE FORWARDED	OFFICER'S INITIALS	COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)
1. General Counsel 7D-01 Headquarters				Tony:
2.				I believe there are significant differences between our interpretation of the language in paragraphs 4 and 5. I still am of the opinion that the present language, even with your suggested amendments, significantly degrades the DCI's authority to establish and maintain special project controls. The language in paragraph 5 was inserted, I believe, to provide NSA with unilateral authority on SIGINT security contrary to the intent of 12036. In view of the above, I have prepared the attached for the Director. I am sure he would appreciate any comments you have on the subject.
3.				
4.				
5.				
6.				
7.				
8.				STATINTL
9.				[redacted]
10.				Robert W. Gambino Att
11.				cc: D/DCI/Support
12.				
13.				
14.				
15.				

FORM 3-62 610 USE PREVIOUS EDITIONS ☐ SECRET ☐ CONFIDENTIAL ☐ INTERNAL USE ONLY ☐ UNCLASSIFIED

MEMORANDUM FOR: Director of Central Intelligence

VIA: Deputy Director of Central Intelligence

FROM: John F. Blake
Deputy to the DCI for Support

SUBJECT: DCI Authority for SIGINT Security Policy [redacted] 25X1

25X1 1. [redacted] Action Requested: None; for your information only.

2. [redacted] Background: E.O. 11652 setting national policy on security classification has been under review leading to revision pursuant to PRM-29. The third and final draft of the proposed new Order was released on 5 April 1978. It includes for the first time in this review/revision process language which would substantially exempt SIGINT security policy matters from DCI control. A copy of Sections 4(e) and 5(b) of its draft order containing this language (italicized) is at Attachment 1. This language was inserted by Defense (Deanne Siemer, General Counsel), at the instance of NSA. The language would:

25X1 a. [redacted] Make the Secretary of Defense responsible, subject to review only by the Director of the Information Security Oversight Office (to be established in GSA by the proposed Order) and by the National Security Council, for setting procedures for the review, declassification, or continued classification of cryptologic information produced by Department of Defense components.

25X1 b. [redacted] Exempt all COMINT special access programs (i.e., compartments) from the periodic DCI review that the Order will require for all other special access programs pertaining to intelligence sources and methods.

25X1 3. [redacted] Discussion: The new language bearing on SIGINT security has the effect of reopening matters settled by E.O. 12036. That Order (Section 1-601(i)) makes the DCI responsible for ensuring the establishment by the Community of common security and access standards for foreign intelligence systems, information and products. Other sections (e.g., 1-601(h) and 1-604(b)) give the DCI other security policy responsibilities.

25X1

[redacted]

SECRET

Authority to review compartmentation procedures to protect SIGINT, and to determine when and how Secret SIGINT information may be released and subject to declassification, is a key element of the DCI's security responsibilities under E.O. 12036.

25X1 4. [redacted] The Defense/NSA language on SIGINT security bears on what the Congress has been told is planned to improve national/tactical interface security. The SECDEF/DCI National/Tactical Report to the Congress stated that "proposed security policy provides for existing special product controls to be used sparingly, and then only for those products and data that reveal particularly sensitive aspects of a program as determined by the DCI" (emphasis added).

25X1 5. [redacted] NSA's reasons for pushing this language appear to reflect:

a. (C) Their sensitivity about any real or perceived diminution of their long-standing authority in the area of SIGINT security. Admiral Inman's letter of 22 July 1977 to the DCI concerning DIRNSA's authority to grant COMINT accesses is an example (Attachment 2).

[redacted] 25X6

25X1 6. [redacted] Deletion from the proposed Executive Order of the Defense/NSA language on SIGINT security would not diminish the degree or type of protection that sensitive SIGINT information would properly receive under national security classification policy. Such deletion would return the proposed new Order to the original agreed approach which would make the DCI responsible for all compartmented security programs bearing on intelligence sources and methods. It would also permit classified cryptologic information to be subject to the same declassification review and action procedures as would apply to other kinds of foreign intelligence data. Elimination of the new language would maintain the integrity of E.O. 12036 with regard to DCI authority for intelligence security policy.

25X1 7. [redacted] The Director of Security has discussed these items with the General Counsel. The latter believes that the offending language in paragraph 4(e) has been effectively eliminated by amendment which he suggested to Mr. Robert Gates, Special Assistant, National Security Council, on 13 April 1978 (copy attached). The General Counsel does not believe paragraph 5(b) diminishes the DCI's authority in any way. Obviously, the Director of Security and the General Counsel are in disagreement concerning these two issues and I believe your personal attention to this matter is warranted.

John F. Blake

Attachments:
1. Extracts of Draft E.O
2. Memo to DCI, dated 22 Jul 1977

SUBJECT: DCI Authority for SIGINT Security Policy [redacted] 25X1

Distribution:
Orig. - DCI w/att.
1 - DDCI w/att.
1 - ER w/att.
1 - C/SECOM w/att.
(1) - General Counsel

SECRET

Section 4. Declassification and Downgrading

(e) Systematic Review for Declassification

(1) Classified information constituting permanently valuable records of the Government as defined by 44 U.S.C. 2103 and information in the possession and control of the Administrator of General Services pursuant to 44 U.S.C. 2107 or 2107 note, shall be reviewed for declassification as it becomes 20 years old. Agency heads listed in Section 2(b), and officials designated by the President pursuant to Section 2(b)(1), of this Order may extend classification beyond 20 years, but only in accordance with Sections 4(c) and 4(e)(2). This authority may not be delegated. When classification is extended beyond 20 years, a date for declassification or the next review no more than 10 years later shall be set and marked on the document. Subsequent reviews for declassification shall be set at no more than 10-year intervals. The Director of the Information Security Oversight Office may extend the period between subsequent reviews for specific categories of information.

(2) Within 180 days after the effective date of this Order, the agency heads listed in Section 2(b) and the heads of agencies which had original classification authority under prior orders shall, after consultation with the Archivist of the United States and review by the Information Security Oversight Office, issue and maintain guidelines for systematic review covering 20-year old classified information under their jurisdiction. These guidelines shall state specific, limited categories of information which, because of their national security sensitivity, should not be declassified automatically but should be reviewed item-by-item to determine whether continued protection beyond 20 years is needed. All information not identified in these guidelines as requiring review and for which a prior automatic declassification date has not been established shall be declassified automatically at the end of 20 years from the date of original classification. These guidelines shall be

authorized for use by the Archivist of the United States and by any agency having [illegible]

(3) Notwithstanding Section 4(e)(1) and (2), the Secretary of Defense may establish special procedures for review and declassification of classified cryptologic information produced by units of the Department of Defense. These procedures shall be reviewed and approved by the Director of the Information Security Oversight Office prior to implementation by the Secretary. The Secretary may appeal any decision by the Director in this regard to the National Security Council. In case of an appeal, the information will remain classified until the appeal is resolved.

(4) Review for declassification of foreign government information shall be in accordance with the provisions of Section 4(c) and with guidelines developed by agency heads in consultation with the Archivist of the United States and, where appropriate, with the foreign government or international organization concerned.

NOTE: Subsection (4) is to be rewritten to make clear that foreign-originated information is subject to a different procedure on declassification review (30- vice 20-year period; an inherent presumption of continuing sensitivity.

Section 5. Safeguarding

(b) Special Access Programs

(1) Agency heads listed in Section 2(b)(1) may create special access programs to control access, distribution, and protection of particularly sensitive information classified pursuant to this or prior Orders. Such programs may be created or continued only by written direction and only by these agency heads or, for matters pertaining to intelligence sources and methods, by the Director of Central Intelligence. Classified information in such programs shall be declassified according to the provisions of Section 4. Special access programs may be created or continued only on a specific showing that:

(i) Normal management and safeguarding procedures are not sufficient to limit need-to-know or access;

(ii) The number of persons who will be reasonably small and commensurate with the objective of providing extra protection for the information involved; and

(iii) The special access controls balance the need to protect the information against the full spectrum of needs to use the information.

(2) All such special access programs *except those required by treaty or international agreement* shall terminate automatically every five years unless renewed in accordance with the procedures in this subsection.

(3) Within 180 days after the effective date of this Order, the agency heads listed in Section 2(b)(1) shall review all existing special access programs under their jurisdiction and continue them only in accordance with the procedures in this subsection. Each of those Agency heads shall also establish and maintain a central list of all special access programs they create or continue. Those agency heads and the Director of the Information Security Oversight Office shall have non-delegable access to all such lists.

NOTE: Last sentence of Subsection (3) is to be deleted.

ATTACHMENT 2

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND 20755

Executive Registry
77-5209

Serial: N0859
22 July 1977

CONFIDENTIAL

MEMORANDUM FOR THE DIRECTOR OF CENTRAL INTELLIGENCE

SUBJECT: Sensitive Compartmented Information Policy

1. Reference NFIB-9.2/59 dated 12 July 1977.

2. The memorandum of reference, received from the Acting Vice Chairman of NFIB, advises me of your 5 July 1977 directive to the Acting Deputy to the DCI for the Intelligence Community, conveying your security policy with regard to Sensitive Compartmented Information. That directive states, with regard to COMINT, that you intend to stabilize the 1 June 1977 level of access until 1 December 1977. It further states that "for each person who is indoctrinated for access to material controlled (in the COMINT system), another person must be removed from access to the same system. I shall expect the number of persons holding such access approvals to be reduced during this freeze period... ."

3. While recognizing and supporting the concern which prompted the policy statement, I believe it could be interpreted to limit the authority of the Director, NSA, to grant access to communications intelligence classified information to persons employed in, or detailed or assigned to the National Security Agency. Authority to grant such access to employees of NSA derives, in part, from Public Law 88-290, and has been delegated to the Director, NSA, by the Secretary of Defense.

4. I am confident your policy statement is not directed at a modification of the established authorities and procedures necessary to the effective operation of NSA. I respectfully request your understanding of the need for me to proceed under these authorities to continue to grant access to new employees as required, with full attention to the spirit of your policy in limiting access to sensitive compartmented data.

STATINTL

B. R. INMAN
Vice Admiral, U. S. Navy
Director

Classified by [illegible]
Exempt from GDS, EO 11652, Cat 2
Declassify Upon Notification by the Originator

Approved For Release 2003/08/08 : CIA-RDP81-00142R000200070006-0

20 April 1978

MEMORANDUM FOR: General Counsel

STATINTL

FROM : [redacted]
Office of General Counsel

SUBJECT : Executive Order on National Security Information

1. Bob Gates called me this morning to discuss our recommendations as to sections 2(e)(1) and 4(d)(1). Contrary to our previous understanding, section 4(d)(1)(ii) is not to be deleted; instead, it is to be modified. By the end of our conversation, however, I was convinced that the language to be placed in the Order is acceptable.

2. First, section 2(e)(1) apparently is to remain as we agreed yesterday; that is, the first clause of the second sentence is to be deleted. As to section 4(d)(1), Rick Neustadt insisted that subparagraph (1)(ii) is to be reinserted but in what I believe is an acceptable form. Section 4(d) is to provide as follows:

> (1) Except as provided in Section 4(e)(4) below, information classified on or after the effective date of this Order shall be declassified or reviewed in accordance with the date or event set pursuant to Section 2(e).
>
> (i) Information not marked with such a date or event shall be declassified automatically six years after the date of original classification, unless the head of the agency extends its classification personally and in writing in accordance with Section 2(e)(2).
>
> (ii) When information is marked for review within six years of original classification pursuant to Section 2(e)(1), and that review is not conducted by the end of the sixth year, the information is automatically declassified; however, the head of the agency or officials authorized to originally classify Top Secret may restore and extend the classification personally and in writing in accordance with Section 2(e)(2) (emphasis added).

In addition, both Gates and Neustadt recognize that the CIA will need considerably more Top Secret classifiers than originally contemplated. The result therefore will be that more Agency employees will be permitted to originally classify

information for years, however, the necessity of establishing a date for review within six years should be considerably diminished because of this increase in Top Secret classifiers; thus, a relatively small quantity of material will be marked for review at the six year period. Sections 2(e)(1) and 4(d)(1) as revised make it clear that classification may be restored and extended subsequent to that time, and are phrased in such a manner as to remove any inference that a six year systematic review will be required. Bob has requested that we indicate whether or not these revisions are acceptable. I believe they are, but that we should indicate our acquiescence with the understanding that the numbers of Top Secret classifiers is not to be limited. I am not totally convinced that the Order now permits as extensive a delegation of Top Secret authority as Gates suggests. Also, section 4(d)(1)(i) is unacceptable.

3. In addition, Bob told me that the Department of Defense is adamant on obtaining an exemption from section 2(f) for the National Security Agency [i.e., Classification Identification and Marking]. Bob is reasonably upset with DoD for raising this matter at such a late date and, while he expects that exemptions could be granted by the ISOO for "specialized" classes of information, he is not disposed towards any blanket exemption.

4. Finally, I met with [redacted] (DDA), [redacted] (DCI Security Committee), and [redacted] (OSO) to discuss the effect of section 4(e)(3) on DCI authorities. All agreed that language permitting the Secretary of Defense to "establish special procedures for review and declassification of classified cryptologic information produced by units of the Department of Defense" will open the door for NSA to compete with the DCI for security control.

STATINTL
STATINTL
STATINTL

5. Briefly, the problem apparently involves primarily the DCI in his Intelligence Community role. Under Executive Order 12036, section 1-601, the DCI is authorized to:

> (h) Conduct a program against overclassification of foreign intelligence information; and
>
> (i) Ensure the establishment by the Intelligence Community of common security and access standards for managing and handling foreign intelligence systems, information and products.

This language, in conjunction with security directives issued by the DCI, establish community-wide security policy. Thus, despite the language in section 1-1202 that no government agency "may engage in signals intelligence activities except pursuant to a delegation by the Secretary of Defense," the DCI is responsible for all SIGINT security policy, including that in the cryptological field. It is believed that NSA wants to dispute this authority. [Note: I have been informed that this language was drafted by NSA and Deanne Siemer over the objections of all other DoD components.]

6. Those present at the meeting viewed the matter as a DCI rather than as a CIA problem. It is generally (although not completely) true that CIA produces cryptological material only pursuant to a delegation from DoD because it controls SIGINT tasking; that is, DoD upon receipt of its requirements will task others who may need NSA assistance in production. As to that information which DoD produces, it has authority to classify and declassify. However, the relevant decisions must be in conformity with security standards established by the DCI. The effect of section 4(e)(3), therefore, might be to permit DoD to establish procedures inconsistent with such standards.

7. It is my opinion that, while the draft should not be interpreted as suggested, the provision could be worded in a way which would, more clearly than it does now, preclude such an inference. Although it may be argued that section 4(e)(3) is unnecessary, there is no objection to permitting DoD to establish special procedures in order to ease its burden of reviewing sensitive cryptological information, especially when it is accepted that such information generally requires protection for more than twenty years anyway. Also, a more politically acceptable approach might be simply to have the ISOO authorize exemptions pursuant to section 4(e)(1). Nevertheless, rather than throw roadblocks in DoD's way needlessly, section 4(e)(3) would be acceptable if modified:

> Notwithstanding Section 4(e)(1) and (2), the Secretary of Defense may establish special procedures for systematic review and declassification of classified cryptologic information produced by units of the Department of Defense. These procedures shall be consistent, so far as practicable, with the objectives of Section 4(e)(1) and (2) and shall be reviewed and approved by the Director of the Information Security Oversight Office and, for matters pertaining to intelligence sources and methods, by the DCI prior to implementation...

Deleted from this version is the inference that the DCI and DoD jointly establish procedures, and added is the clear intent to ensure that DCI authorities not be affected. Tactical cryptological information will remain solely within DoD control. Alternatively, a more extreme approach might be to permit the "DCI, in consultation with the Secretary of Defense" or the "Secretary of Defense, consistent with security standards established by the DCI" to establish special procedures. This surely will be unacceptable to Defense but might serve as a useful starting point. In any event, language more clearly recognizing DCI equities is not undesirable.

8. Let me repeat that the language as drafted, limited as it is to systematic declassification and review, does not authorize DoD to establish procedures in any way inconsistent with authorized DCI policies. The existence of a possible loophole, however, suggests an amendment is in order for section 4(e)(3). As to section 5(b)(2), however, I remain convinced that no amendment is needed.

That section troubles the Office of Security because it is believed that the exemption as to special access programs established pursuant to international agreement will effectively shield DoD intelligence compartments from DCI review, although the language provides an exemption only as to automatic termination every five years. There is no restriction on the DCI's reviewing such programs as well. To clarify this point, the following language might be useful:

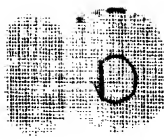
> (2) All special access programs regularly shall be reviewed and, except those required by treaty or international agreement, shall terminate automatically every five years unless renewed in accordance with the procedures in this subsection.

I believe this raises an issue which Gates may wish to have resolved only by the President, but it might be useful at this point to use this as a means for the DCI to strengthen his community role. In this regard note E.O. 12036, section 1-601 that the DCI shall:

> (g) Formulate policies concerning intelligence arrangements with foreign governments, and coordinate intelligence relationships between agencies of the Intelligence Community and the intelligence or internal security services of foreign governments.

Review by the DCI of compartments established pursuant to agreements with foreign services seems to be appropriate under this section, and it may be appropriate, although not essential, to force the issue.

STATINTL



Approved For Release 2003/08/08 : CIA-RDP81-00142R000200070006-0

26 April 1978

MEMORANDUM FOR: General Counsel

STATINTL VIA : [redacted]

STATINTL FROM : [redacted]
Office of General Counsel

SUBJECT : Executive Order on National Security Information: Section 4(e)(3)

1. On 25 April 1978 I again met with representatives of DDA and DDS&T in order to discuss the impact of section 4(e)(3) as proposed by the Department of Defense. As a result of this meeting I continue to maintain that, while the proposal should not affect DCI authorities as feared by DDA, the provision could be worded in a way which would, more clearly than it does now, preclude the offending inference.

2. The justification provided by Deanne Siemer has not completely satisfied the DDA that the DCI's authorities are not intended to be affected. The stated purpose to section 4(e)(3) is to relieve NSA of a burdensome item-by-item review of classified information to determine whether continued protection beyond 20 years is needed. This section, however, could provide an exception for any review at all at the 20 year period if appropriate procedures are approved by the ISOO. The DoD justification that it intends to issue procedures that "provide for continued classification beyond 20 years for all or nearly all signals intelligence" could be interpreted to permit DoD to protect information despite a DCI decision to review and declassify.

3. A second, perhaps more important, consideration involves the fact that these special procedures promulgated by the Secretary of Defense shall apply to information "produced by" units of the Department of Defense. It is my understanding that information is collected, processed, disseminated to and analyzed by appropriate intelligence agencies which publish the final product, i.e., intelligence. As early as at the collection stage, however, information may be deemed produced so that, presumably, any information collected by DoD and placed in NFAC reports or studies, as well as anything derived therefrom, will be subject to the DoD procedures. The concern expressed by DDA at the meeting

was that sources and methods information contained in these intelligence reports would be out of the control of the DCI by virtue of these procedures. However, DDS&T observed that the DCI really has no control of such information today, but establishes overall security standards. It was agreed, however, that DoD should be asked to explain further what information DoD expects to be covered by these procedures.

4. There was some recognition that the placement of section 4(e)(3) in the section pertaining to systematic review and declassification thereby limits the scope of any DoD procedures. Thus, DDS&T could accept the DoD language since the DCI standards and criteria for classification and declassification continue to apply, and DoD procedures must be consistent. The DDA, however, believed that the interests of the DCI would be better served by refusing to accept the DoD language and that, at a minimum, DCI approval of DoD procedures applicable to intelligence sources and methods should be required to preclude any adverse inferences.

5. The final point raised in Deanne Siemer's memorandum is that the special procedures for cryptological information would be more marketable coming solely from NSA rather than appearing to be a "community-wide project taking advantage of a large loophole." The response to this argument, however, is that CIA information should be protected to the same degree as DoD's. It must be noted that DoD's objection was to a provision which we no longer consider necessary if alternative language is acceptable. A requirement to cover CIA information as well is not needed. A preferable provision would be to require approval of special procedures by the ISOO and, for matters pertaining to intelligence sources and methods, by the DCI. Permitting the DCI to approve procedures in no way creates any loophole; rather, it merely recognizes that the DCI has responsibilities regarding intelligence sources and methods. It was generally thought at the meeting that DoD could have no objection to such an addition if it were forthright in its justification provided to us. Any objection from DoD could be interpreted as bad faith.

6. In conclusion, DDS&T is more willing to accept the DoD explanation for its proposal, although it desires further clarification on how these procedures are to affect NFAC reports. Also, DDS&T wants assurances that the classification requirements are not affected and that DCI standards for classification and declassification are still applicable. On the other hand, DDA is more skeptical and urges our recommended language in order to preclude any adverse inference of DoD control over intelligence sources and methods. That position would hope to prevent any possibility of DCI ineffectiveness in the face of procedures promulgated pursuant to the Order and approved by the ISOO; i.e., it would nip DoD villainy in the bud.

7. My opinion is that section 4(c)(3) as proposed by DoD is acceptable when read in context, first with the rest of the Order and, second, with Executive Order 12036 and applicable NSCIDs. It would not be inappropriate, however, to ask Deanne Siemer if our present amendment, which she has not seen, is acceptable. Since it creates no "large loophole" as did our previous language, I would be interested in hearing the rationale for any further opposition. Finally, failing acceptance of our amendment, we may attempt to clarify the provision by means of the implementing directive.

[redacted] STATINTL